NOT FOR PUBLICATION UNTIL RELEASED BY
THE SENATE ARMED SERVICES COMMITTEE
CYBERSECURITY SUBCOMMITTEE

STATEMENT BY

VICE ADMIRAL MICHAEL M. GILDAY

COMMANDER

U.S. FLEET CYBER COMMAND

U.S. TENTH FLEET

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

CYBER POSTURE

2ND SESSION 115TH CONGRESS

MARCH 13, 2018

NOT FOR PUBLICATION UNTIL RELEASED BY
THE SENATE ARMED SERVICES COMMITTEE
CYBERSECURITY SUBCOMMITTEE

Chairman Rounds, Ranking Member Nelson and distinguished members of the Subcommittee, thank you for your continued support of the men and women of U. S. Fleet Cyber Command, U.S. TENTH Fleet, and the United States Navy. It is an honor and privilege to represent the outstanding Sailors and civilians who comprise our U.S. Fleet Cyber/U.S. TENTH Fleet team, and I appreciate this opportunity to update you on how our Navy's cyberspace operations are evolving to remain competitive in today's strategic environment.

As discussed by the National Defense Strategy, great-power competition has reemerged as the central challenge to U.S. security and prosperity. It will probably come as no surprise to this committee that our adversaries often act within the "gray zone," heavily relying on asymmetric methods such as cyberspace and information operations to undermine our national interests.

Over the past four years, as the Commander of U.S. Fleet Cyber Command and as the former Director of Operations for U.S. Cyber Command, I have observed first-hand how the United States is threatened by cyber-attacks every day; the threat to the U.S. Navy is certainly no different. Our ability to command and control our forces relies upon cyberspace. Virtually every operation aboard a Navy ship - navigation, engineering, communications and weapons employment – rests on the secure and reliable transfer of and confidence in our data. Operating in the maritime environment does not shield us from the threats inside of the cyberspace domain, and our competitors know this. The cyberspace domain is a great capability leveler due to the low cost of entry for adversaries who desire to achieve an effect against us. With interconnectedness and pervasiveness increasing due to the Internet of Things, this environment will only become more complex and contested.

And beyond today's threats, our current technological advantages are not preordained. We are in an unprecedented age of exponentially accelerating technology and a convergence of technologies that brings dynamic and innovative capabilities. The technological race is on for Artificial Intelligence, Machine Learning and Quantum Computing as the world's most powerful militaries strive to become the leader in these areas. Maintaining our role as a global superpower requires us to develop and evolve our cyber capabilities quickly to dominate in this technologically advanced environment.

In the same fashion that the historic U.S. TENTH Fleet from World War II enabled the prosecution of the U-Boat threat and ensured access to the shipping lanes of the Atlantic, U.S. Fleet Cyber Command and the modern U.S. TENTH Fleet exists today to enable, anticipate and prosecute cyberspace threats and ensure our Navy networks supporting our most critical missions are protected and ready.

Since its establishment on Jan. 29, 2010, U.S. Fleet Cyber Command /U.S. TENTH Fleet has grown into an operational force comprised of more than 16,000 active duty Sailors, reserve component Sailors and civilians assigned to 29 active duty and 29 reserve commands around the globe. U.S. Fleet Cyber Command reports directly to the Chief of Naval Operations as an Echelon II command and is responsible for operating and securing Navy Enterprise networks, defending all Navy networks, operating our global telecommunications architecture, and providing cryptology, signals intelligence (SIGINT), cyberspace, and space warfighting capabilities to support Fleet Commanders and Combatant Commanders. With distinct, but

overlapping mission sets, U.S. Fleet Cyber Command serves as the Navy Component Command to U.S. Cyber Command for cyberspace operations, the Navy's Service Cryptologic Component Commander under the National Security Agency/Central Security Service and the Navy's component for space under U.S. Strategic Command.

Headquartered in Fort Meade, Maryland., U.S. Fleet Cyber Command exercises operational control of globally-deployed Cyber Mission Forces (CMF) through a task force structure aligned to the U.S. TENTH Fleet. U.S. Fleet Cyber Command is also designated as the Joint Force Headquarters-Cyber aligned to U.S. Pacific Command and U.S. Southern Command for the development, oversight, planning and execution of full spectrum cyberspace operations aligned with other traditional warfighting lines of operations.

In 2015, U.S. Fleet Cyber Command released its *Strategic Plan: 2015-2020*, which identified five goals critical to deliver on our responsibilities by leveraging our strengths and shrinking the Navy's cyber-attack surface to cyber adversaries, which I will detail throughout this statement. Across the wide-ranging responsibilities, our five goals are:

1. Operate the Network as a Warfighting Platform: Defend Navy networks, communications and space systems, ensure availability and, when necessary, fight through them to achieve operational objectives.
2. Conduct Tailored Signals Intelligence: Meet the evolving SIGINT needs of Navy commands, including intelligence support to cyber.
3. Deliver Warfighting Effects Through Cyberspace: Advance our effects delivery capabilities to support a full spectrum of operations, including cyber, electromagnetic maneuver, and information operations.
4. Create Shared Cyber Situational Awareness: Create a shareable cyber common operating picture that evolves to full, immediate awareness of our network and everything that happens on it.
5. Establish and mature Navy's Cyber Mission Forces: Stand up 40 highly expert CMF Teams and plan for the sustainability of these teams over time.

We, the Navy and U.S. Fleet Cyber Command/U.S. TENTH Fleet, have made significant progress towards these goals, continue to develop organizationally and evolve to outpace competitors. On behalf of the warfighters of U.S. Fleet Cyber Command, I thank you again for opportunity to discuss the Navy's progress in cyberspace and our course ahead.

Operate the Network as a Warfighting Platform

The Navy, like other DoD and government entities, faces enormous challenges in cyberspace. Foreign governments and non-state actors use cyberspace operations as an integral part of their national and military strategies. Adversaries take advantage of publicly available cyber tools so nefarious actors can quickly identify vulnerabilities in software and hardware to exploit high priority targets.

In May 2017, a cyber-attack known as WannaCry spread ransomware rapidly and indiscriminately across the world. The malware encrypted and rendered useless hundreds of

thousands of computers in hospitals, schools, homes, and businesses in over 150 countries. In June 2017, numerous commercial ships transiting coastal waters in the Black Sea reported having their GPS systems "spoofed," so that their locations were reported inside Russian territorial waters, as opposed to being in international waters.

These examples demonstrate we operate in an increasingly contested cyber environment where information is the fuel of decision making and protecting that information and our mechanisms for Assured Command and Control (C2) are critical to successful maritime operations. Loss of this information, or lack of confidence in the veracity of the information we see, not only degrades our confidence and effectiveness of our C2, it also leads to loss of intellectual property and removes our competitive edge. The margins of victory are razor thin, and we cannot afford to lose a step.

U.S. Fleet Cyber Command/U.S. TENTH Fleet approach to overarching cyber defense is consistent with U.S. Fleet Forces Command's *Fleet Design* and the Chief of Naval Operation's plan for a Future Navy, with more innovation across the Fleet. The networks upon which the Navy depends to conduct its missions and fight effectively are presently under continuous probing, if not outright attack by determined adversaries. Simply put, any system with embedded information technology or networking capability is a target for an adversary. Technology is increasingly moving in the direction of everything defaulting to being networked so this environment will continue to increase in complexity and pose challenges to our operations.

U.S. Fleet Cyber Command directs operations to secure, operate, and defend Navy networks, which currently consists of more than 500,000 end user devices; an estimated 75,000 network devices (e.g., routers, servers); and approximately 45,000 applications and systems across multiple security enclaves. These systems are comprised of information technology, combat and operational technology and control systems. I can most succinctly capture our approach to cybersecurity by stating the Navy operates all of its networks as warfighting platforms. As a warfighting platform it must be aggressively defended from intrusion, exploitation and attack. As a warfighting platform, the network must be agile, resilient, and responsive to the C2, intelligence, logistics, and combat support functions that depend upon it. As a warfighting platform, its configuration must also be precisely maintained. It must be resilient to attack and allow us to "fight through the hurt." Finally, as a warfighting platform, it must be capable of and available to deliver warfighting effects in support of Combatant Commander operational priorities.

Reflective of the larger culture, the demand for seamless connectivity continues to grow, and solutions to visualize and protect this operational key terrain must keep pace. The Fleet must have trust and confidence in its networks, systems and data, and the information and knowledge they present. Failure to adequately protect and assure our Fleet networks would be detrimental to our maritime operational capability and warfighting effectiveness. Therefore, the importance of a secure architecture for Navy networks cannot be overemphasized. Our Systems Commands, Program Executive Offices (PEOs) and government research centers play a pivotal role in design and acquisition of our systems. Their focused R&D efforts of secure, resilient architectures and systems, reinforced by industry and academia best practices, are needed to ensure we are investing in the right systems, technologies and methodologies to provide a resilient information

environment that can be operated and maintained by our personnel. Effective systems engineering also highlights the importance of ensuring our cybersecurity processes are intertwined with our network capabilities so we can maintain proper cybersecurity controls. Designing, developing, testing and fielding systems resilient to cyber exploitation is a key step in this. As the Navy Authorizing Official (NAO), we serve as a the oversight authority through utilization of the DoD Risk Management Framework to ensure new systems include the proper cybersecurity controls and identification of risk on our networks from design through fielding, and most importantly throughout their operating lifecycle.

Additionally, U.S. Fleet Cyber Command is operationally focused on continuously improving the Navy's cyber security posture through an emphasis on the combination of people, process and technology. This allows us to reduce the network intrusion attack surface, implement and operate layered defense in depth capabilities, and expand the Navy's cyberspace situational awareness as outlined below.

Reducing the network intrusion attack surface

Opportunities for malicious actors to gain access to our networks come from a variety of sources such as known and zero-day cyber security vulnerabilities, poor user behavior, and supply chain vulnerabilities. Operationally, we think of these opportunities in terms of the network intrusion attack surface presented to malicious cyber actors. The greater the size of the attack surface, the greater the risk to the Navy mission. The attack surface grows larger with aging operating systems and when security patches to known vulnerabilities cannot be rapidly deployed across our networks, systems, and applications.

The Navy is taking positive steps in each of these areas to reduce the network intrusion attack surface including enhanced cyber awareness training for all hands, enhancements to how we monitor our networks for compliance and vulnerabilities, reducing the time to field patches and fixes, and improving the process on how we inspect the cyber readiness of our networks.

An example of an innovative approach to reducing our attack surface is our Continuous Hardening and Monitoring Program (CHaMP) initiative. CHaMP brings together current and historical information from all sources, Navy attack surfaces and network operations to focus our network and operational system hardening and remediation efforts. The program aims to include continuous machine-assisted assessments of Navy commands' vulnerability management compliance, Information Assurance accreditation status, and network owner responsiveness in securing their networks. Based on threat indicators and command performance relative to Navy and DoD cybersecurity standards, the CHaMP program will be used to prioritize the assignment and deployment of our Navy Blue Team and other cybersecurity response activities. Furthermore, we are bolstering our ability to manage cyber security risks in our networks by closely integrating our access and authorized activities with operations and risk-based inspections. This allows us greater understanding of IT challenges and configuration management processes. Through our work with industry partners and academia we are exploring ways to utilize data analytics, machine learning, and other automation technologies to do some of the cybersecurity heavy lifting that will bring our defensive posture to the next level.

Additionally, the Navy is reducing the attack surface with significant investments and consolidation of our ashore and afloat networks with modernization upgrades.

The Navy's Next Generation Enterprise Network- Recompete (NGEN-R) is an evolution building on the successes of the current ashore enterprise contracts (Navy Marine Corps Intranet and OCONUS Network (ONENET)). By incorporating lessons-learned from Operation ROLLING TIDE in 2013, a large-scale network maneuver and operation to eradicate an adversary from the Navy's unclassified network, and combining our overseas and CONUS shore enterprise networks under NGEN-R we can improve situational awareness, and our ability to C2, and operate and defend Navy networks. The enhanced situational awareness capability of NGEN-R will enable our headquarters and network defense forces to make better informed network operational decisions, and improve speed and agility to maneuver our networks for maximum effectiveness.

Often times, people are viewed as the largest vulnerability in this equation – by that same logic, our people, each and every person touching a keyboard, can make the network stronger. We believe a Navy cyber defense is an all hands effort like damage control on a ship. Our entire Navy needs cyber training but not everyone requires the same level of instruction. So we have developed tailored cyber training for our cyberspace workforce, leaders, average users and those who require escalated privileges. All Navy personnel are required to complete online cybersecurity awareness training upon hiring or accession, with an annual refresher. For the cyberspace workforce, the Navy is providing training that enables them to effectively conduct cyber offensive and defensive operations. Like other warfighting lines of operation, cyberspace operations training is also being delivered to an increasing number of officers via their professional military education, as well as in undergraduate and graduate school curriculum. The Navy addressed the need to integrate cyber training in other leadership development courses as well throughout the ranks. Finally, systems and operational commands identified enhanced users who require specialized cybersecurity training based on the roles they perform. For example, certain engineers at the systems commands will receive cybersecurity training so they are able to build better defend their unique networks and systems. Some of this training is already underway. An example of an operational enhanced user would be select shipboard technicians trained to recognize cyber threats to their operational technology/industrial control systems and recover them from attacks against those systems.

Enhance our Defense in Depth Operations

The Navy is working closely with U.S. Cyber Command, NSA/CSS, our Cyber Service counterparts, DISA, Inter-Agency partners, and commercial cyber security providers to enhance our cyber defensive capabilities on all of our networks through layered sensors and countermeasures including the interface with the public internet on our unclassified networks down to the individual computers that make up our Navy networked environments. Key to this is our ability to detect and react to adversary activity and restore capability quickly. These defensive measures are informed by all source intelligence and industry cyber security products combined with knowledge gained from analysis of our own network sensor data. As information sharing improves, so does the shared responsibility for mutual defense.

From the long-haul communications that form our wide area network backbones to software and infrastructure purchased as a service such as commercial cloud, we are dependent upon commercial industry and share our cybersecurity responsibilities in partnership with them. While the rise of dual-use technology has created vulnerabilities, it has also created opportunities for us. Many of our challenges are not unique to the .mil domain and are shared by commercial industry. We fend off the same cast of adversaries, who are using the same tactics, techniques and procedures within .edu, .gov and .com domains. We work similarly to reduce the attack surface by applying countermeasures and patching known vulnerabilities on the same types of network infrastructure. Industry is and will remain a critical mission partner through technology development, sharing lessons learned, sharing risks, and responsible intelligence sharing.

As industry evolves capabilities we can employ, we include those in our overall architecture, and we are currently piloting and deploying new sensor capabilities to improve our ability to detect and respond to adversary activity as early as possible. In the future, we see industry advances in the fields of Artificial Intelligence (AI) and machine learning will allow us to continually improve the tools we employ on our networks to enable a more predictive and automated cyber defensive environment. It's a fast paced fight. We need to respond faster than the adversary and envision automation as the means to outpace the threat. This includes increasing the diversity of sensors on our networks, moving beyond strictly signature-based capabilities to behavioral sensing, and improving our ability to proactively detect new and unknown malware. We need these tools to help us sense what is "normal" and detect what activity on the network is just outside that, so we can act quickly. Capable adversaries will operate at or below the "noise level" so using the advanced analytics enabled by AI and machine learning will give us a tactical advantage in identifying malicious activity early. We are working with partners to investigate the best way to use these data science technologies for mission assurance.

At the tactical edge, 17 of our 20 Cyber Protection Teams are deployed around the globe today as well as five afloat Defensive Cyberspace Operations (DCO) teams deployed within our Carrier Strike Groups and Amphibious Ready Groups. We are leveraging big data analytics, as well as machine learning to improve our ability to protect that data in our networks. We also work closely with our Navy systems commands (SYSCOM) , such as Naval Sea Systems Command (NAVSEA), Naval Air Systems Command (NAVAIR), and Space and Naval Warfare Systems Command (SPAWAR), for example, in order to protect our weapon systems and platforms from cyber-attacks. Each of the Navy systems commands provides full life-cycle support for a specific category of military hardware or software, including research and development, design, procurement, testing, repair, and in-service engineering and logistics support. Our partnerships with the SYSCOMS help to expand our cyberspace situational awareness and protecting our assets effectively.
The Navy continues to support the spirit and intent of the Joint Information Environment (JIE), including the implementation of a Single Security Architecture (SSA) that begins with the Joint Regional Security Stacks (JRSS). The Navy and Marine Corps Intranet is our primary onramp into JIE, including incorporating JIE technical standards into the acquisition of the Navy Enterprise Networks as those standards are defined. In parallel, the Navy is setting internal technical standards for implementation of a Defense in Depth functional architecture across all our systems commands and networks, afloat and ashore – from standard desktop services to combat systems and industrial control systems. Additionally, the Navy is well into the transition

along with the rest of DoD to the Risk Management Framework, which is drawn from a solid basis using National Institute of Standards and Technology practices. This is significant as it moves us from an antiquated compliance focus perspective to one of risk focus informed by intelligence, providing improved cybersecurity, a concept we are applying to all of our networks IT, industrial controls and Combat Systems. Most importantly, we are integrating ways to better understand operational cybersecurity risk and defensive posture throughout an information system's life cycle. Operations in cyberspace are highly dynamic; we can only achieve a truly defensible architecture by investing in automation of the collection, integration, and presentation of data built in from the beginning as an integral part of each system. These actions will help us to truly build cybersecurity and resilience in initial system design and development and avoid the pitfalls associated with trying to bolt them on at the end. Continuous monitoring is critical to our understanding of how consistently our systems are properly configured in accordance with standards. Only then can operational commanders make cyber maneuver decisions with confidence that they will deliver the intended results.

JRSS will become part of our future defense in depth capabilities. As described above, the Navy has already consolidated our networks behind defensive sensors and countermeasures. We expect that JRSS v2.0 will be the first increment connected to the Navy Enterprise Networks. Accordingly, the Department of Navy is planning to consolidate under JRSS 2.0 as part of the technical refresh cycle for NMCI when JRSS meets or exceeds existing Navy capabilities. Integrating the Navy Enterprise Network with the JRSS will allow shared visibility into the boundary capabilities for Navy and DOD.

As we make improvements in our monitoring of Navy networks, we will continue to feed that operational picture into the JIE joint environment to ensure shared situational awareness across DOD of the Navy's portion of the Department of Defense Information Networks as a risk to one is shared by all.

For our part, U.S. Fleet Cyber Command is operationally focused on continuously improving the Navy's cyber security posture by reducing the network intrusion attack surface, implementing and operating layered defense in depth capabilities, and expanding the Navy's cyberspace situational awareness.

Create Cyber Situational Awareness

Just like any other domain, success in cyberspace requires awareness of both ourselves and our enemies. It requires that we constantly monitor and analyze Navy platforms within both the classic maritime system and global information system. The Navy continues down the acquisition path to expand our Navy Cyber Situational Awareness (NCSA) capabilities with a more robust, globally populated and mission-tailorable Cyber Common Operating Picture (COP). A new capability under development called SHARKCAGE will provide us significantly improved analytics and speed of response by leveraging the power of machine learning. In parallel, we are establishing the organizational linkages required giving context to that picture and our data strategy focuses on seamless integration with all DoD network operations, industrial controls, and maritime operations data. For example, we are collaborating with Navy Facilities Command (NAVFAC) to include sensor feeds from industrial control systems into our NCSA,

informing operators of the cyber defensive status of critical infrastructure systems for a more holistic view for mission assurance.

U.S. Fleet Cyber Command Operational Forces

Status of the Cyber Mission Force

The CMF has three primary missions: Defend the nation against national level threats, support combatant commander missions, and defend Department of Defense information networks.

Navy teams are organized across existing U.S. Fleet Cyber Command operational commands at cryptologic centers, fleet concentration areas, and Fort Meade, depending upon their specific mission. Navy is responsible for sourcing four National Mission Teams, eight Combat Mission Teams, and 20 Cyber Protection Teams, and for their supporting teams consisting of three National Support Teams and five Combat Support Teams.

Given the dynamic nature of the cyber environment, our Navy CMF teams have achieved and must sustain a high degree of readiness. All 40 of the Navy-sourced CMF teams achieved Full Operational Capability (FOC) as of October 6th, 2017, one year ahead of the designated U.S. Cyber Command target. Navy CMF teams are currently actively engaged in cyber offensive and defensive operations globally as part of the joint force.

FOC is an externally validated evaluation indicating the unit has met all its capability requirements and can perform its mission as designed. However, it is not a measure of combat readiness. Achieving FOC was only a waypoint as the Navy's operational need for a well-trained and motivated cyber workforce will continue to grow in the coming years. Although reaching this milestone is a great accomplishment, the true challenge is in sustaining that high degree of readiness and the ability to promptly 'answer all bells' when directed by U.S. Cyber Command. We are meeting that readiness challenge through continuous execution of current operations, a robust training program and in ensuring our forces have the tools and infrastructure they need to succeed.

Additionally, we have focused on the integration of our Fleet's efforts, capacity and capabilities across the Navy and Joint force. In my role as the Joint Force Headquarters-Cyber commander aligned to U.S. Pacific Command and U.S. Southern Command, this is an area where organizationally we have made significant progress last year.

Our planning with U.S. Pacific Command must be robust enough to create cyber support plans that are integrated into their operational plans in the more traditional warfighting areas. This requires a staff that is fully embedded into the supported combatant commander processes while being synchronized with my main staff at the Headquarters at Fort Meade. As a JFHQ-C Commander, I directed an extension of my staff in February 2017 to integrate at U.S. Pacific Command and provide cyberspace planning and force employment into operations alongside forces from the other warfighting domains. We organized our CMF teams, which included three US Air Force CMF teams and two US Army CMF teams, as well as my Navy CMF teams, in Hawaii to form an interim Cyber Forward Element as a one-stop-shop for full spectrum

cyberspace operations in support of U.S. Pacific Command. This extension of my staff provides Offensive and Defensive Cyberspace planning to PACOM until a permanent Cyber Operations-Integrated Planning Element, or CO-IPE, is in place. A CO-IPE, serves as the forward extensions of Joint Force Headquarters – DODIN and Joint Force Headquarters-Cyber. We are in the process of standing up three permanent CO-IPE at PACOM, SOUTHCOM and US Forces Korea, working with our combatant commanders to project power in, from and through cyberspace. These Elements will also fully integrate cyberspace into battle plans, ensuring timing and tempo are set by the commanders for use of cyberspace effects in the field based on their operational scheme of maneuver.

Reserve Cyber Mission Forces

Through ongoing mission analysis of the Navy Total Force Integration Strategy, we developed a Reserve CMF Integration Strategy that takes advantage of our 298 Reserve Sailors' skill sets and expertise to maximize the Reservist support for full spectrum cyber operations. These Reservists are being brought into service through FY18, and will be individually aligned to Active Duty CMF teams and the Joint Force Headquarters-Cyber. In this way, we can employ the unique skillsets our Reserve Sailors bring to the fight, while building a cadre of highly trained personnel that can be ready for surge efforts now and in the future.

As our Reserve Cyber billets are fully manned and these personnel trained over the next few years, we will continue to assess our Reserve CMF Integration Strategy and adapt as necessary to develop and maintain an indispensably viable and sustainable Navy Reserve Force contribution to the CMF.

We are also exploring relationships with academia by establishing reserve detachments with high-performing academic research institutions. For example, this past year, we have directed and resourced the creation of a reserve detachment (FCC/C10F Det Pittsburgh), attached to Navy Cyber Warfare Development Group (NCWDG), whose mission is to better leverage the research and technology rising out of Carnegie Mellon University (CMU) and Software Engineering Institute (SEI) in Pittsburgh, PA. This was initiated to better connect with advances in the academic world in order to enhance our cyber mission force training and cyber tool development.

Recruit and Retain

In FYs 2016 and 2017, the Navy met officer and enlisted cyber accession goals, and is on track to meet accession FY18 goals in May of 2018. Currently authorized special and incentive pays, such as the Enlistment Bonus, should provide adequate stimulus to continue achieving enlisted accession mission, but the Navy will continue to evaluate their effectiveness as the cyber mission grows.

Today, Navy Cyber Mission Force (CMF) enlisted ratings (CTI, CTN, CTR, IS, IT) are meeting retention goals. Sailors in the most critical skill sets are eligible for Selective Reenlistment Bonus (SRB). SRB contributes significantly to retaining our most talented Sailors, but we must closely monitor its effectiveness as the civilian job market continues to improve and the demand

for cyber professionals increases. Additionally, Navy is reviewing whether additional incentives for our most critical skill sets, such as Interactive On-Net Operators (IONs), are warranted.

Cyber-related officer communities are also meeting retention goals. While both Cryptologic Warfare (CW) and Information Professional (IP) communities experienced growth associated with increased cyber missions, we are retaining Officers in these communities at 93 percent overall. Both CW and IP are effectively-managing growth through direct accessions and through the lateral transfer process, thereby ensuring cyber-talented officers enter and continue to serve. Additionally, since 2011, the Navy has 40 Cyber Warfare Engineers (CWE) in the ranks, the Navy's direct commission program for experienced and highly talented cyber professionals.

Fortunately, the Navy has had seen a sufficient quantity and quality of individuals via our established accession means (USNA, ROTC, OCS, direct commissions, etc.) for CW, IP, CWE and Cyber Warrant Officers (CWO) communities. Leveraging special authorities granted by Congress as the time is not necessary (10 U.S. Code 533(g). However, as the "War for Talent" continues due to the combination of an upward trending economy and an ever increasing competition for cyber skillsets, this authority will allow the Navy to remain competitive in the future as necessary.

With respect to the civilian workforce, we currently have 91 civilian positions within the Cyber Mission Force. Forty-seven of these positions are filling various work-roles throughout the CMF and the remaining 44 are our Computer Scientists/Tool Developers. Currently we have 27 of the 47 positions filled throughout CMF; we continue to recruit for our 44 Tool Developers and have made 17 selections to date, and have 12 personnel onboard. We are aggressively hiring to our civilian authorizations consistent with our operational needs. Our primary challenges in recruiting are the current compensation allowable and competition with industry and other DoD entities. With this in in mind, we are currently offering various incentives to potential candidates which includes higher step (step 7) on the GS pay scale, 10% of salary as a one-time recruitment incentive, 10% of salary for relocation expenses, and several years of assistance in student loan payback (5K per year). Even with these incentives, we are not competitive with industry or the National Security Agency (NSA), and we intend to increase these incentives in the near future. Additionally, we are optimistic that the Cyber Excepted Service implementation (Phase II) will help in our recruitment efforts. We plan to use all of the authorities available to us and hire to our Cyber positions, to include our JFHQ-C and CO-IPE, as expeditiously as possible.

As the economy continues to improve, we expect to see more challenges in recruiting and retaining our cyber workforce.

Educate, Train, Maintain

The Navy currently manages, under the Executive Agent appointment of the Cryptologic Training System, the Joint Cyber Analysis Course, which provides basic initial accession (1000-level training) skillsets for Cyber operations used by all services, including acting as the accession school for the Navy's Cryptologic Technician Networks rate. Further, Cyber and Information Security knowledge in accession are maintained in training for the Information Systems Technology rate and recently added basics for the Intelligence Specialist accession path.

Officers in Cryptologic Warfare and Information Professional designators receive Cyber and Information Security requirements.

As directed in the NDAA of FY16 and in close consultation with U.S. Cyber Command, the Navy is on tracking towards to begin resourcing training for Sailors assigned to its CMF in FY19. As also outlined in the January 2017 Cyber Force Model Training Transition Plan for foundational (2000-level) training, the Navy is prepared to execute administrative oversight of designated cyber training curriculum in FY19. 2000-level training for Navy organic Information Systems Technicians providing Information Assurance and Network Security functions are in place through Navy channels. Similar training for Navy organic operational Network Defense personal is conducted on an individual basis with future plans to transition to a systematic approach.

U.S. Cyber Command mandates Joint Cyberspace Training and Certification Standards for the CMF, which encompass procedures, guidelines, and qualifications for individual and collective training. Most of the training today is delivered by U.S. Cyber Command and the National Security Agency (NSA) in a federated but integrated approach that utilizes existing schoolhouses and sharing of resources while Sailors are in an operational status. Through the CFMTT plan with resourcing, the services will transition to providing Sailors that have already received foundational training. CMF training specifically involves 54 role-specific, intermediate through advanced training pipelines using a mix of nearly 100 Joint, NSA National Cryptologic School (NCS), and multi-Service courses to prepare officers, enlisted and civilians for their CMF work roles. These training events are not only aimed at the individual Sailors, but also provide operational team certifications and sustainment training. Once certified, our team training is maintained throughout the year via several key unit level exercise events which allow individuals and the collective team to demonstrate required skills against simulated adversaries. U.S. Fleet Cyber Command/U.S. TENTH Fleet augments the required U.S. Cyber Command training pipeline in two ways--- online skills development and the provision of supplemental academics.

Using the DoD's Enterprise Cyber Range Environment (DECRE) resources, provided by the Joint Staff, U.S. Fleet Cyber Command utilizes Joint Information Operation Range nodes (JIOR) to connect CMF teams with ranges which are representative of shipboard networks. These networks are used as offensive and defensive mission rehearsal platforms and to augment individual training for various team work-roles. U.S. Fleet Cyber Command has also invested in a web-based individual and collective training platform, using a commercial virtual environment, to augment the academic portions of the U.S. Cyber Command training pipeline with hands-on skills development. The Persistent Cyber Training Environment (PCTE), managed by the Department of the Army, is expected to incorporate similar distributed training methodologies in module- based systems. When necessary, teams seek out and receive additional training based on work roles or specific mission requirements.

From a formal educational perspective, to develop officers to succeed in the increasingly complex cyberspace environment, the Navy offers the following opportunities for cyber development:

- *USNA*: The U.S. Naval Academy offers introductory cyber courses for all freshman and juniors to baseline knowledge. Additionally, U.S. Naval Academy began a Cyber Operations major in the Fall of 2013. Furthermore, the Center for Cyber Security Studies harmonizes cyber efforts across the U.S. Naval Academy.
- *NROTC*: Our Naval Reserve Officer Training Corps' program maintains affiliations at 51 of the 180 NSA Centers of Academic Excellence at colleges around the country. Qualified and selected graduates can commission as Information Warfare Officers, Information Professional Officers, or Intelligence Officers within the Information Warfare Community.
- *NPS*: For graduate-level education, the Naval Postgraduate School offers several outstanding graduate degree programs that directly underpin cyberspace operations and greatly contribute to the development of officers and select enlisted personnel who have already earned a Bachelor's Degree. These degree programs include Electrical and Computer Engineering, Computer Science, Cyber Systems Operations, Network Warfare Operations and Technology, and a masters of Applied Cyberspace Operations.
- *NWC*: The Naval War College (NWC) is also incorporating cyber into its strategic and operational level war courses, at both intermediate and senior graduate-course levels. NWC also integrates strategic cyber research into focused Information Operations IO/Cybersecurity courses, hosts a Center for Cyber Conflict Studies (C3S) to support wider cyber integration across the College, and has placed special emphasis on Cyber in its war gaming role.

Together with U.S. Naval Information Forces, we will be realigning several of our operational commands to stand-up an Information Warfare Training Group (IWTG) later this month. This new command will advance IW readiness and warfighting capabilities, including Cyberspace Operations (CO), through training, assessments and certification assistance for Type Commanders in order to prepare afloat and shore activities to face the challenges of a dynamic threat environment.

Future Cyber Workforce Needs

The Navy's operational need for a well-trained and motivated cyber workforce (active, reserve and civilian) will continue to grow in the coming years. We continue to analyze the readiness of our Cyber Mission Force and will adjust recruiting tools, as required.

U.S. Fleet Cyber Command/U.S. TENTH Fleet is partnered with University of Maryland's "Center for the Advanced Study of Language" (CASL) in researching aptitude assessments for our cyber workforce. Cyber workforce screening and recruitment may be aided by the refinement and implementation of the Cyber Aptitude and Talent Assessment (CATA). The CATA will enhance screening and selection of the individuals best suited for specific work roles and assist with vectoring personnel into the work roles where they have the best probability of success, potentially reducing the training pipeline, minimizing attrition and delivering the most capable workforce. Assuming success with ongoing developmental efforts, we will work with stakeholders to identify logical injection points. (Recruiting, Universities, Service Academies, etc).

Fleet Readiness

The Navy's 2019 budget continues to prioritize readiness alongside the investments necessary to sustain an advantage in advanced technologies and weapons systems. Ensuring the cyber resiliency of networks is part of maintaining the readiness of warfighting platforms.

The budget continues funding to train and equip the CMF, provides investments in Science and Technology and information assurance activities to strengthen our ability to defend the network. To maintain our advantage in advanced technologies and weapons, funding is provided for engineering to improve control points and boundary defense across Hull, Machinery & Electrical, Navigation and Combat Control Systems and for Cyber Situational Awareness.

The Navy requested accelerated funding for procurement of Cyber Protection Teams (CPT) field deployable computing and analysis capability called Deployable Mission Support Systems (DMSS) in PB 18. The procurement and sustainment of 40 DMSS kits is required by Navy Cyber Protection Teams (CPT) to conduct intensive, computationally-heavy analysis when reach back capability is unavailable or bandwidth is limited. Without accelerated funding, this will reduce the number of full-capability DMSS kits available to Navy CPTs and delay the program schedule by over one year. Operationally, this will drive the need to share a limited number of DMSS kits for missions that may occur across the globe. The PB19 request builds upon this effort and will significantly improve operational defensive cyber capability and readiness. Our total inventory objective of sustained DMSS kits is 40, which is projected to occur by 2021.

The Navy is requesting increased investment in Defensive Cyber Operations forces' ability to detect adversary activities and analyze cyber-attacks against Maritime Cyber Key Terrain (CKT) and to integrate all-source intelligence and Navy data to assess adversary capabilities. The goal of these investments is to improve the Navy's capacity to deliver to Operational Commanders, cyber situational awareness at all layers of the IT infrastructure and provide a cyber COP at our Fleet Maritime Operations Centers.

Continued funding for training is necessary to ensure operator proficiency as Fleet systems are modernized and become more complex. I believe the Navy's ability to appropriately fund training of our operators in these new technologies will improve operational readiness.

Summary

The proliferation of cyber capabilities, coupled with new warfighting technologies, will increase the incidence of "gray zone" operations against our Nation and our Navy. Over the past year and a half, we have seen information become a weapon of choice amongst our competitors. We view the information environment to include the domains of space, cyberspace and the electromagnetic spectrum, all merged together as key in our ability to get in front of our adversaries to deny them operational advantages. That invisible battle space is an area that we must optimize to win in the future.

The opening rounds of the next conflict will likely be in cyberspace - the Navy must be ready to prevent wars as well as win them. Therefore, we will conduct operations in and through

cyberspace, the electromagnetic spectrum and space to ensure Navy and Joint/Coalition freedom of action and decision superiority while denying the same to our adversaries. The Navy is closely aligned with U.S. Cyber Command, Combatant Commands, joint and interagency partners, and other Services to support a whole of government response to cyber threats. We will continue to succeed by leveraging our strengths and shrinking our vulnerabilities. We will win in these domains through commitment to excellence and by strengthening our alliances across the US government, Department of Defense, academia, industry, and with foreign partners.

Thank you again for this opportunity to update you on the great work being done by the men and women of U.S. Fleet Cyber Command, U.S. TENTH Fleet and the U.S. Navy. I look forward to working closely with members of the subcommittee on cybersecurity and appreciate your support of the cyber investments included in the Navy's 2019 budget request. I'm happy to take your questions.